TRENDS IN QUANTUM INFORMATION AND COMPUTATION

Francesco De Martini
Università “La Sapienza”
e Sezione I.N.F.M., Roma

Les Rencontres de Physique de La Vallée d'Aoste,
La Thuile 9-15 march 2003

What is computed by the Quantum Computer ?

Answer: GLOBAL PROPERTIES of any function f(x).

Examples:

(a) D.Deutsch (1985): $f(x):\{0,1\} \rightarrow \{0,1\}$

determine whether: $f(0) \oplus f(1) = 0$ or 1

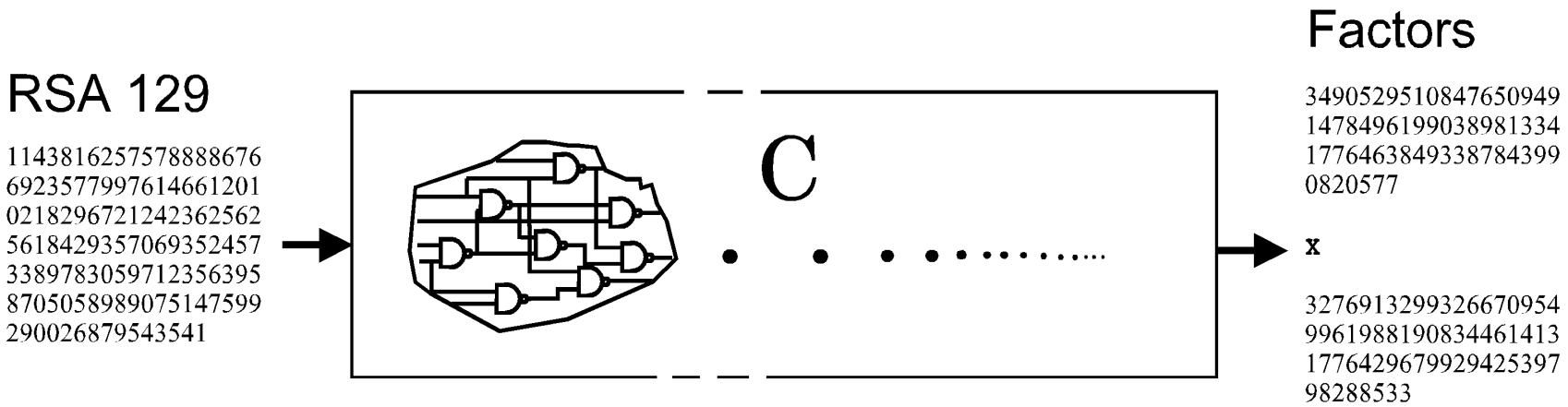
(i.e. if f(x) is *constant* or *balanced*: Adopted algorithm: 2-way Q.Interferometer (IF) = 2 Hadamard-transfs. + 1 phase-transf.)

(b) P.Shor (1994): Factoring any number N

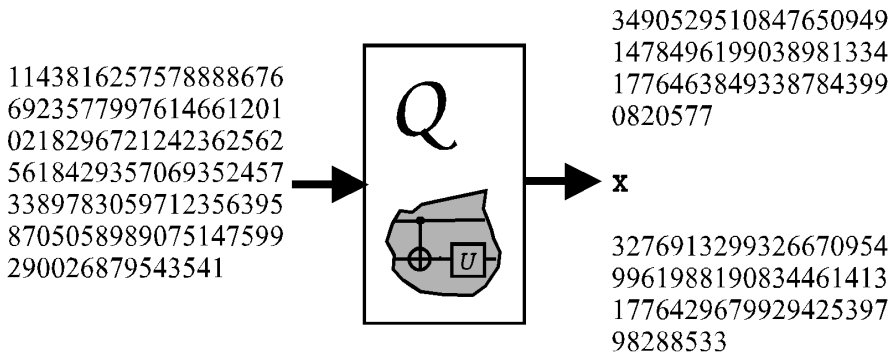
(Adopted algorithm: Quantum Fourier Transform (QFT): *exponential* $\rightarrow$ *polynomial* computation time! $\rightarrow$ RSA 129)

Fast Quantum Computation

Classical factoring problem required 8 months on hundreds of computers



Same Input and Output, but Quantum processing of intermediate data gives



Exponential speedup for Factoring

Quadratic speedup for Search

Example of factoring : **N = pq = 35**

(1) Select any whole number $a<N$, coprime with N (i.e. no common factors $\neq 1$). e.g. do select here: $a = 4$.

(2) Evaluate: $\mathbf{f_{a,N}(x) = a^x \bmod N} \rightarrow f_{4,35}(x) = 4^x \bmod 35 =$ 1,4,16,29,11,9, ,1,4,16,29,11,9,1,4,16,29,11,9,1….

Period of $f_{4,35}(x)$: $r = 6$

(1) Evaluate: $\mathbf{a^{r/2} \bmod N} \rightarrow 64 \bmod 35 = 29$

(4) Gcd $(29 \pm 1, 35) \rightarrow$ gcd (30, 35) = $5 = p$; gcd(28, 35) = $7 = q$

“GLOBAL” PROPERTY of $f_{a,N}(x) \rightarrow$ PERIOD r

By QFT algorithm r is determined in a polynomial time: O(m log m) !

e.g. for key cryptographic system by Rivest, Shamir, Adleman: RSA 129

Quantum Computing: It isn't just factoring!

- Grover search – appointment scheduling
- period finding – group theory computations
- quantum simulation
- Raz algorithm – distributed simulation
- sampling complexity: disjoint subsets
- finite-round interactive proofs
- "pseudo-telepathy" (Bell inequalities, game playing)
- quantum cryptography
- quantum data hiding & secret sharing
- quantum digital signature
- precision measurements & frequency standards
- frame or direction agreement

BUT, some computations are not sped up at all!

See DiVincenzo & Loss, arXiv.org/cond-mat/9901137

Main problem for Q.Computation:

DE-COHERENCE

The decoherence-time T_D of a system, e.g. a IF network, decreases fastly with the system's dimensionality (i.e. # of degrees-of-freedom, including environment)

This leads to a practical impossibility of any "macroscopic quantum coherent system"

or: **SCHROEDINGER-CAT**

DECOHERENCE TIMES OF PHYSICAL SYSTEMS IN TYPICAL ENVIRONMENT

	T_D	T_{op}	$N_{op} = T_D / T_{op}$
Nuclear spin	$= 10^{-2}$-10^{8}	$= 10^{-3}$-10^{-6}	$= 10^{5}$-10^{14}
e^- - spin	$= 10^{-3}$	$= 10^{-7}$	$= 10^{4}$
Ion Trap (In^+)	$= 10^{-1}$	$= 10^{-14}$	$= 10^{13}$
e^- in Gold	$= 10^{-8}$	$= 10^{-14}$	$= 10^{6}$
e^- in GaAs	$= 10^{-10}$	$= 10^{-13}$	$= 10^{3}$
Quantum dot	$= 10^{-6}$	$= 10^{-9}$	$= 10^{3}$
Optical Cavity	$= 10^{-5}$	$= 10^{-14}$	$= 10^{9}$
μ-wave Cavity	$= 10^{0}$	$= 10^{-4}$	$= 10^{4}$

DE-COHERENCE AFFECTS THE COHERENCE OF THE:

(a) Quantum Bit (QUBIT): In 2-dim. Hilbert Space

$$|\Psi\rangle = (\alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle) \qquad |\alpha|^2+|\beta|^2=1$$

(b) Entangled State: In 2×2 dim. A⊗B Hilbert Space

$$|\Psi\rangle = (\alpha\,|\uparrow\downarrow\rangle + \beta\,|\downarrow\uparrow\rangle) \equiv$$

$$(\alpha\,|\uparrow\rangle_A\otimes|\downarrow\rangle_B + \beta\,|\downarrow\rangle_A\otimes|\uparrow\rangle_B)$$

For $\alpha = -\beta = 2^{-½}$ $|\Psi\rangle$ is the "singlet" to be used in tests of violation of Bell's inequalities.

Quantum Entanglement with photons

polarization (spin) π-entanglement, momentum $\mathbf{k}$-entanglement, energy ω-entanglement, angular momentum $\mathbf{L}$-entanglement

Entanglement (E) $\rightarrow$ "..I would not call that *one* but rather *the* characteristic trait of quantum mechanics (QM), the one that enforces its entire departure from the classical lines of thought…"

[E. Schroedinger, Proc.Camb.Phil. Soc. 31, 555 (1935)]

E.P.R. : 2 separated systems (1, 2): described by 2 sets of basis eigenvectors of (non-communting) observables:$\{\varphi, \theta\},\{\chi, \eta\}$:

$$|\Psi> = \Sigma_k \varphi_k(1)\, \theta_k(2) = \Sigma_h \chi_h(1)\, \eta_h(2)$$

PRACTICAL QUANTUM-INFORMATION (QI) REALIZATIONS IN COMPUTATION AND COMMUNICATION

1) Quantum State Teleportation (Roma, 1997)

   a most complex QI network, realized with polarization-entangled-states of optical photons.

1) Quantum Cryptography (1994)

   realizes eavestropping-free communication: commercial system realized with opt.photons.

QUANTUM INFORMATION

AN EXCEPTIONAL TRAINING FIELD FOR MODERN QUANTUM MECHANICS

DISCOVERY OF FUNDAMENTAL BOUNDS IN QI, e.g. in QUANTUM MEASUREMENT: Examples:

1) NO-SIGNALING : NO superluminal communication, i.e.: relativistic causality in (nonrelativistic) Q.Mechanics.

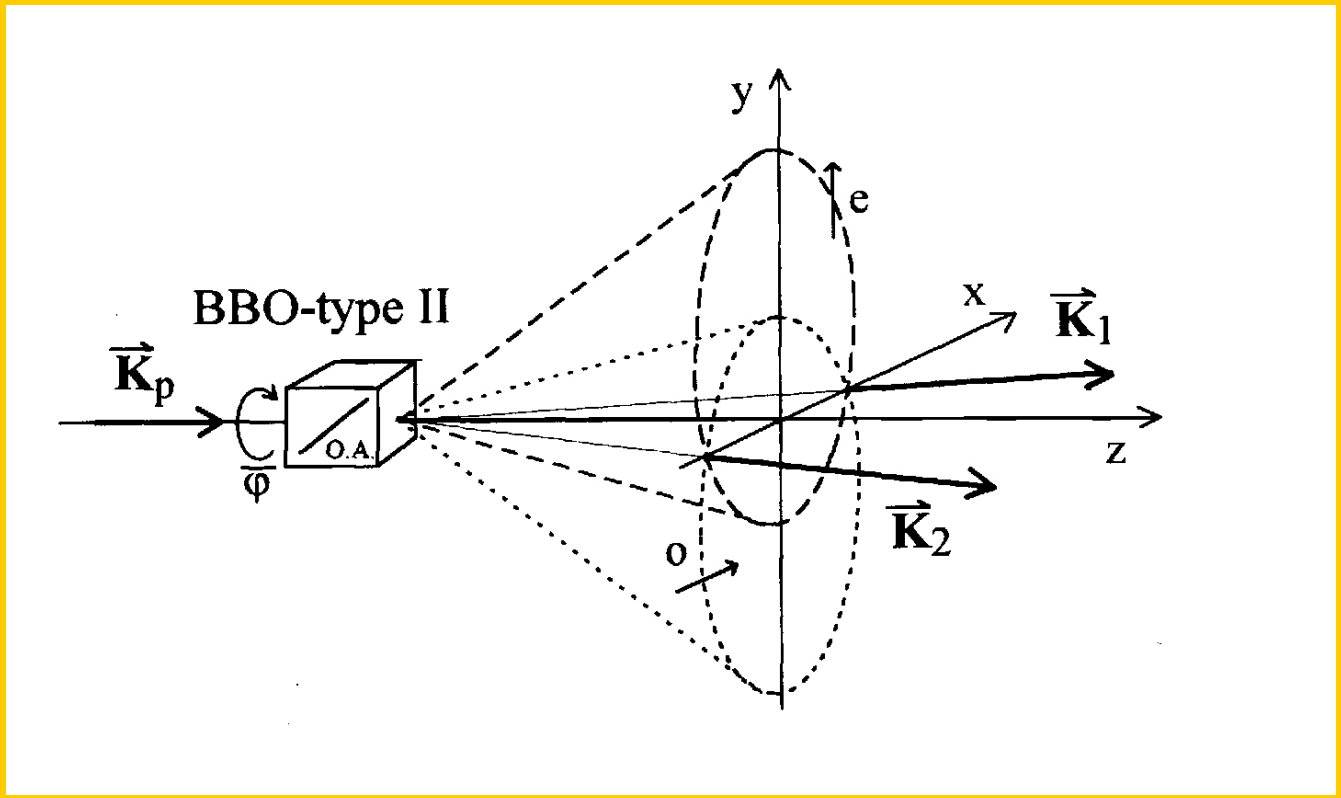
   [Because: any QM operation is a *linear-map*]

2) NO-CLONING THEOREM [QM: *linear-map*]

3) IMPOSSIBILITY of any UNIVERSAL NOT-GATE, i.e. forbidden realization of any time-reversal operation

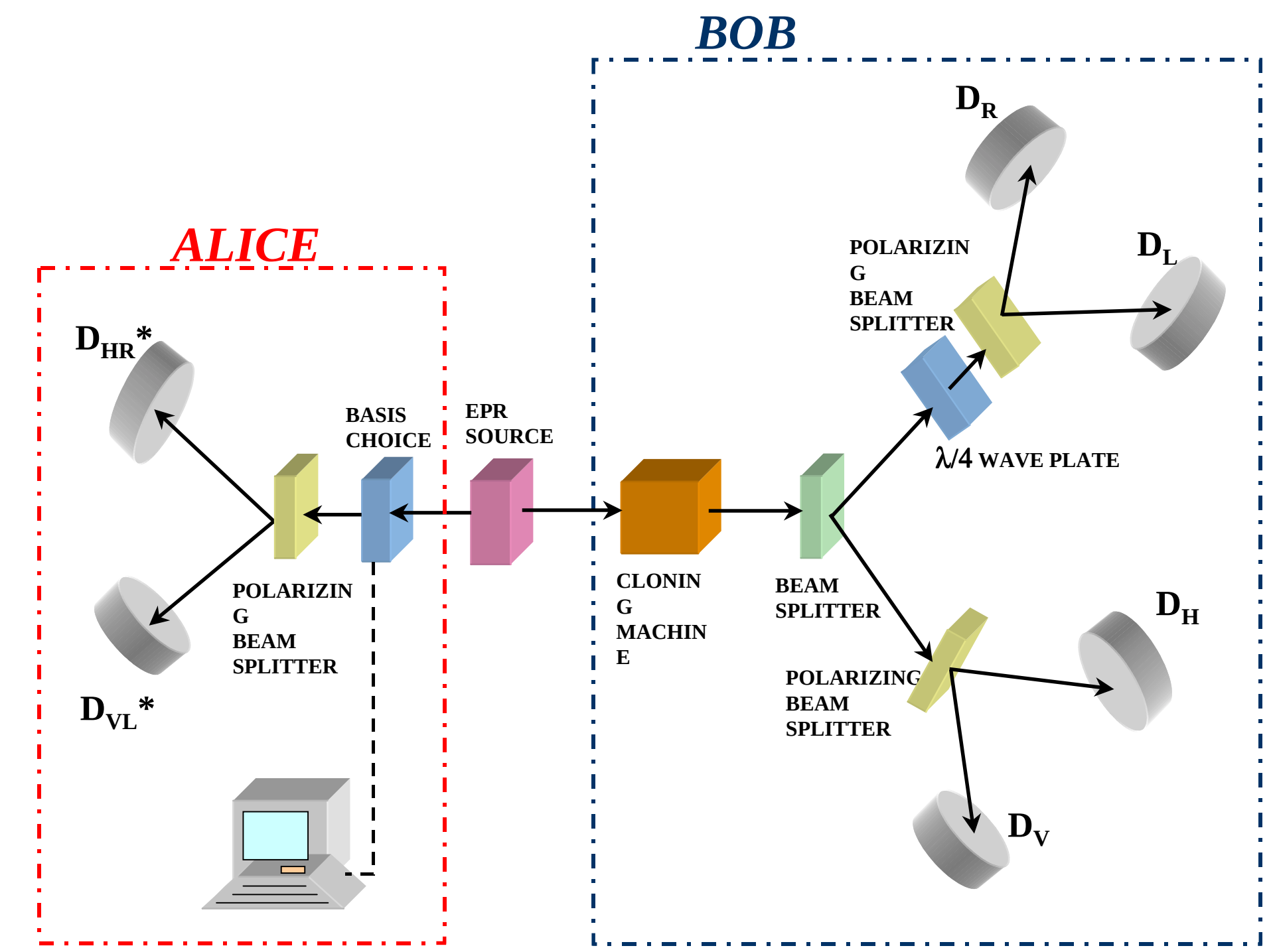
   [QM: *completely positive-map* (CP-map)]

ENTANGLED CONFIGURATION: α–BETA-BARIUM-BORATE (BB0)



On mode K_1 : field operators $\hat{a}_1 \equiv \hat{a}_{1\perp}, \hat{b}_1 \equiv \hat{a}_{1=}$

On mode K_2 : field operators $\hat{a}_2 \equiv \hat{a}_{2=}, \hat{b}_2 \equiv \hat{a}_{2\perp}$


BOB
ALICE
D_R
D_L
POLARIZIN
G
BEAM
SPLITTER
D_{HR}*
BASIS
CHOICE
EPR
SOURCE
λ/4 WAVE PLATE
POLARIZIN
G
BEAM
SPLITTER
CLONIN
G
MACHIN
E
BEAM
SPLITTER
D_H
POLARIZING
BEAM
SPLITTER
D_{VL}*
D_V

Is it really possible to use the quantum nonlocal correlations to establish superluminal communication

between A and B ? (*)

NO, because of the NO-CLONING THEOREM

Implied by the *linearity* of Q.M.

BUT perfect no-superluminal communication by:

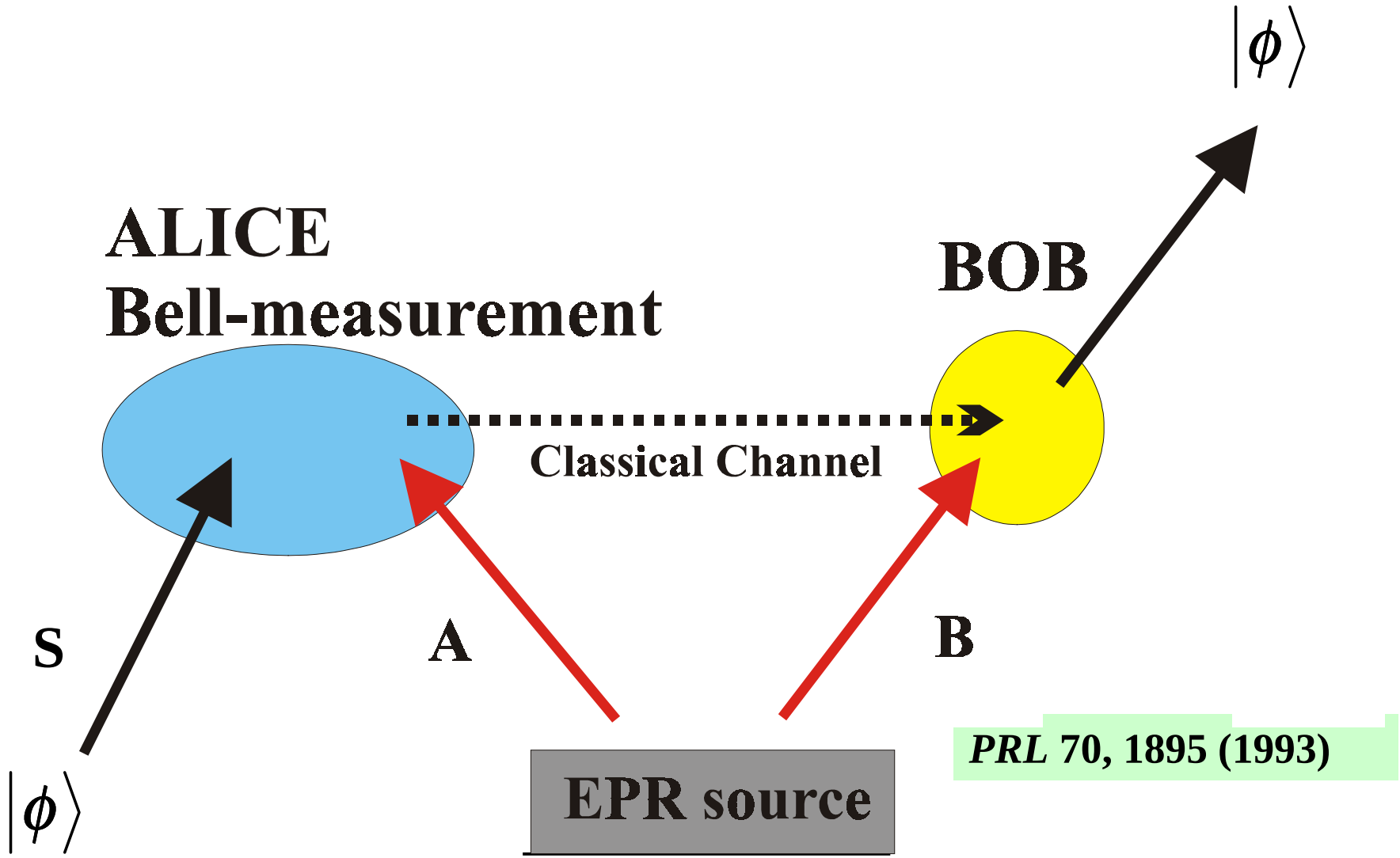
QUANTUM STATE TELEPORTATION !

1. G.C.Ghirardi, Referee Report for Founds.of Phys. 1981 to paper by N.Herbert)

2. W.Wootters and W.K.Zurek, NATURE, 299, 802 (1982)

(*) As suggested by N.Herbert, Found.of Physics, 1982.

Quantum Teleportation



PRL 70, 1895 (1993)

THE LINEARITY OF Q.M. FORBIDS THE REALIZATION
(i.e.with FIDELITY F=1) OF THE

UNIVERSAL QUANTUM CLONING MACHINE (**UQCM**)
I.E. OF THE FOLLOWING PROCESS:

$$|\Psi\rangle\ldots|\Psi\rangle\otimes|\Phi\rangle \Rightarrow |\Psi\rangle|\Psi\rangle\ldots|\Psi\rangle\otimes|\Phi\rangle'$$

FOR **N arbitrary input states** $|\Psi\rangle$ **M > N output states**

1) G.C.Ghirardi, RReport to N.Herbert (Founds.of Phys)1981

2) W.K.Wootters, W.K.Zurek, Nature, 299, 802 (1982)

BUT WE MAY REALIZE A “OPTIMAL” UOQCM WITH “OPTIMAL” FIDELITY $F < 1$:

$$F \equiv (NM + M + N)/(MN + 2M)$$

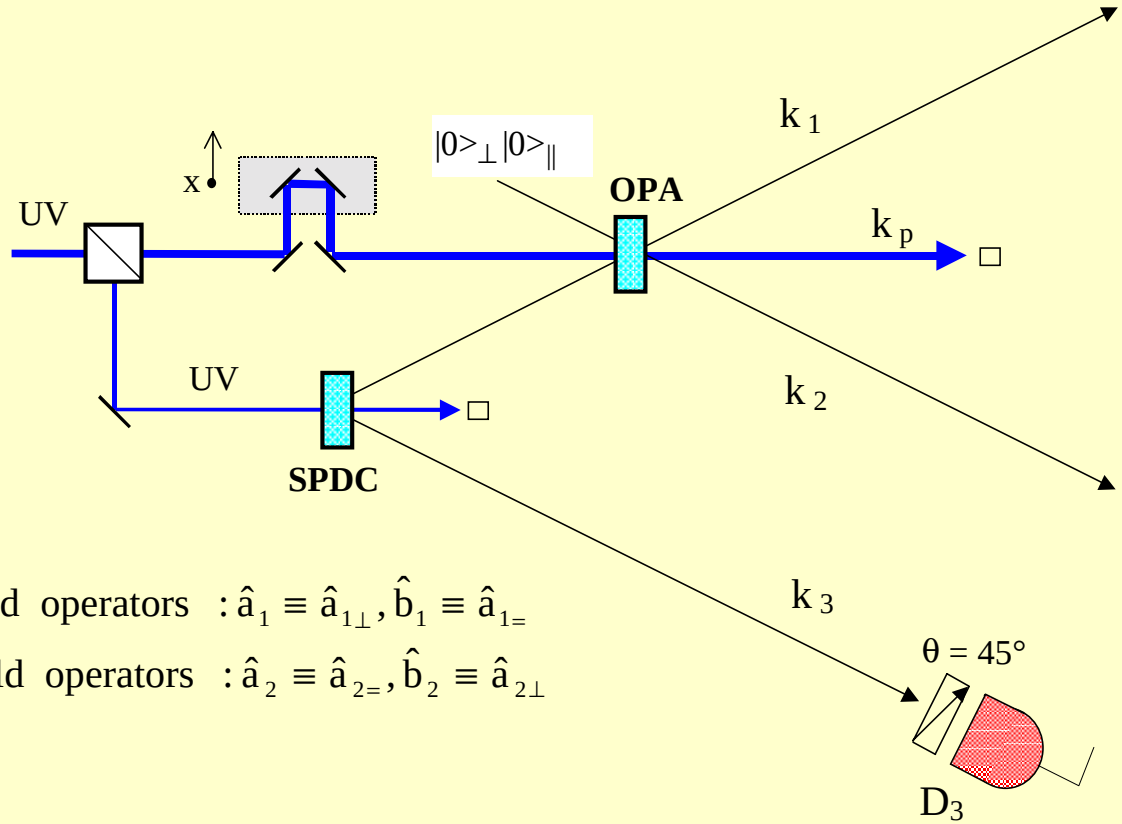
= (relative probability of exact cloning)

N [M] = N^0 input [output] particles

THIS CAN BE REALIZED BY THE QUANTUM INJECTED OPA (FOR N=1, M=2 F = 5/6= 0.833)

QUANTUM INJECTION OF A QUBIT ON MODE K_1

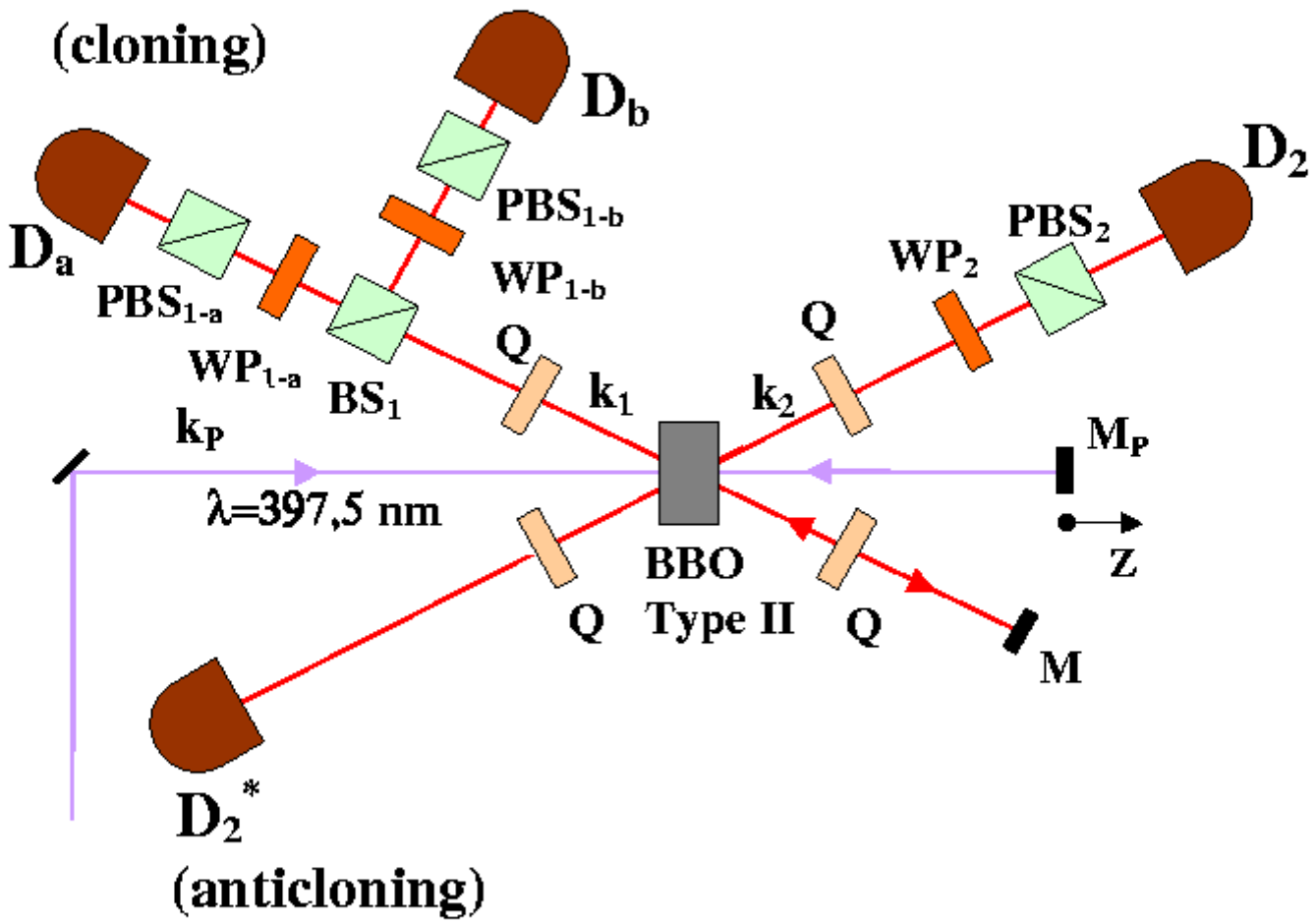
$|\Psi\rangle = \{\alpha|1\ 0\rangle_1 + \beta\,|1\ 0\rangle_1\} \otimes |0\rangle_{2\perp}\,|0\rangle_{2=}$ $\qquad \alpha|^2 + |\beta|^2=1;\ |1\ 0\rangle_1 \equiv |1\rangle_{1\perp}\,|0\rangle_{1=}$

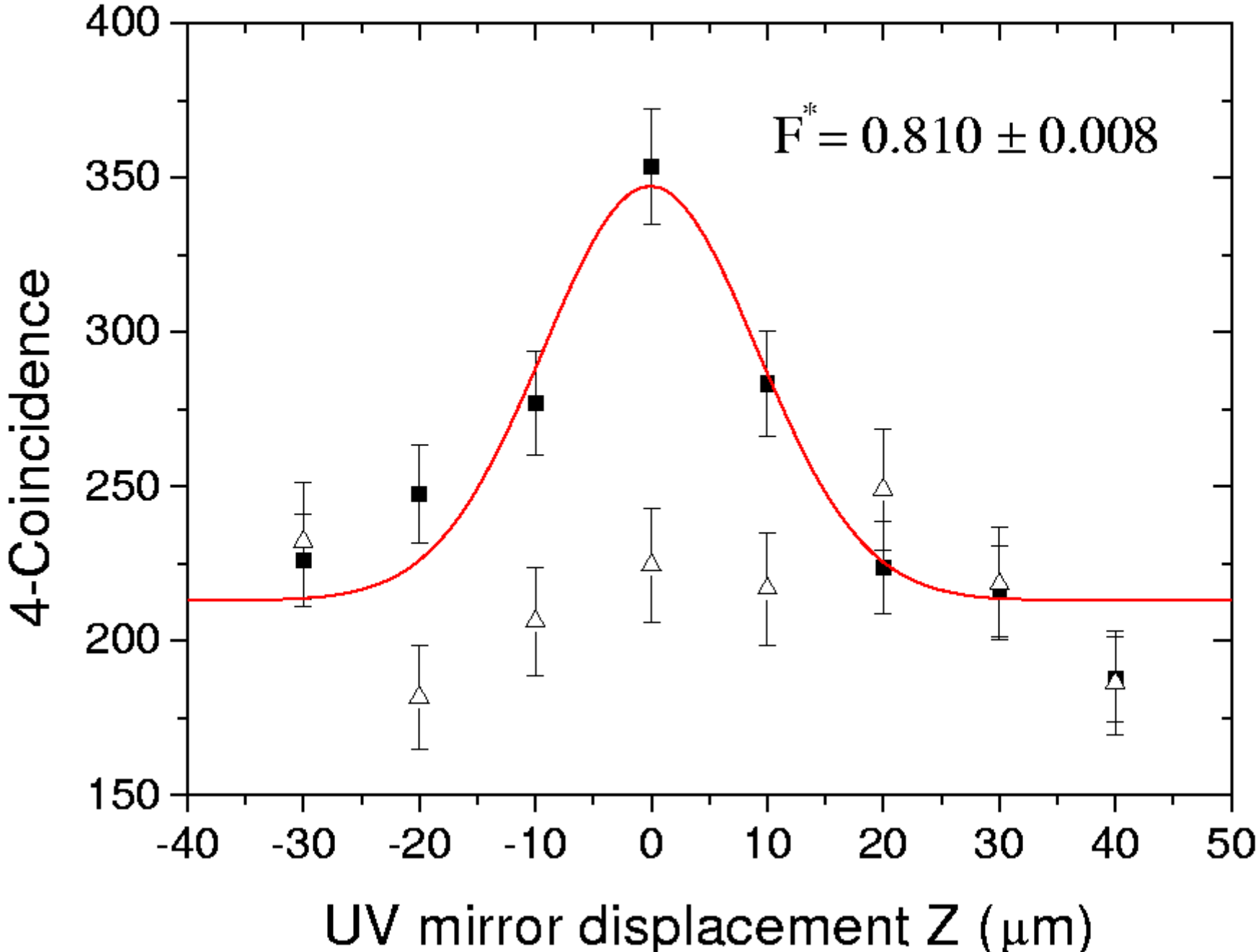


On mode k_1, field operators : $\hat{a}_1 \equiv \hat{a}_{1\perp}, \hat{b}_1 \equiv \hat{a}_{1=}$

On mode k_2, field operators : $\hat{a}_2 \equiv \hat{a}_{2=}, \hat{b}_2 \equiv \hat{a}_{2\perp}$

F. De Martini, P.R.L. 81,2842 (1998)


(cloning)
D_b
D_a
PBS_{1-b}
PBS_{1-a}
WP_{1-b}
WP_{1-a}
BS_1
Q
k_1
k_2
Q
WP_2
PBS_2
D_2
k_P
λ=397,5 nm
M_P
Z
BBO
Type II
Q
Q
M
D_2^*
(anticloning)


400
350
300
250
200
150
4-Coincidence
$F^{*} = 0.810 \pm 0.008$
-40
-30
-20
-10
0
10
20
30
40
50
UV mirror displacement Z (μm)

IMPERFECT CLONING (F < 1)
OR NOT-GATE

- PHYSICAL MODEL: OPA SPONTANEOUS EMISSION (i.e. Vacuum field Amplification)

- BRIDGE BETWEEN QUANTUM PHYSICS AND ELECTRICAL ENGINEERING:

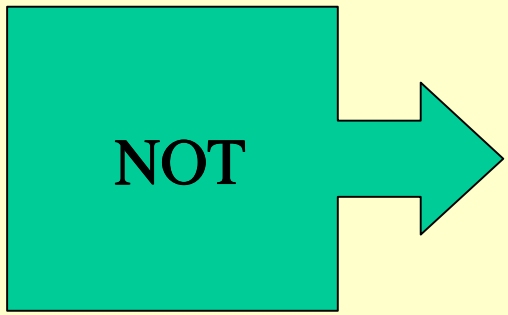
Vacuum field $\Rightarrow$Noise in Parametric Amplifiers.

Vacuum field $\Rightarrow$Source of QM Uncertainties.

UNIVERSAL NOT-GATE
flipping of a qubit on the symmetric point of the Bloch sphere

$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

$|\alpha|^2+|\beta|^2=1$



$|\Psi^{\perp}\rangle = T\,|\Psi\rangle =$

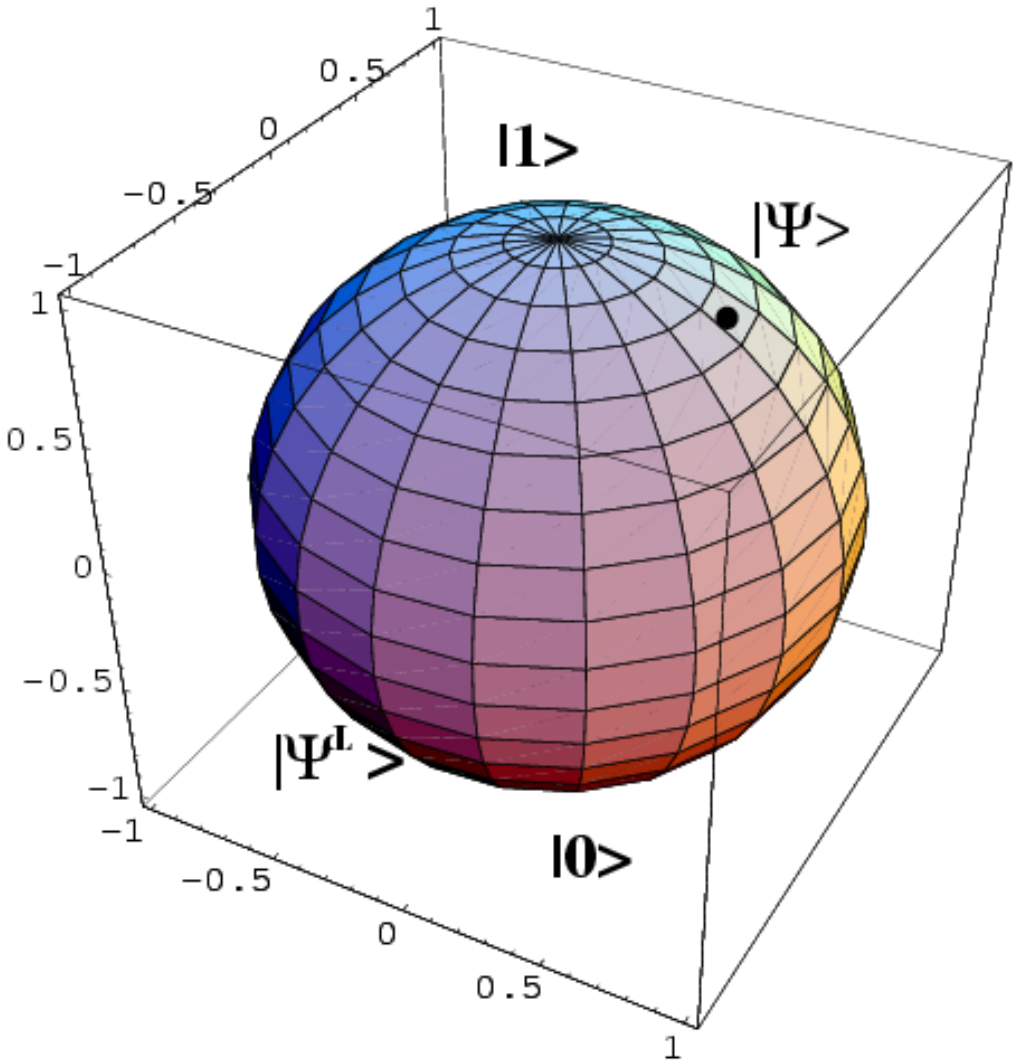
$= \beta^*\,|0\rangle - \alpha^*\,|1\rangle$

$\langle\Psi|\Psi^{\perp}\rangle = 0$

T: time-reversal transformation:
anti-unitary viz. not physically realizable with F=1 !

N.Gisin and S.Popescu, PTL 83, 432 (1999)
V.Buzek, M.Hillery and R.F.Werner, PRA 60, R2626 (1999)
F. De Martini et al, NATURE (2002)

Bloch sphere



OPA UO NOT-GATE

$$\rho_{out} = (2/3)\ |\Psi^{\perp}\rangle\langle\Psi^{\perp}| + (1/3)\ I$$

NOT-GATE FIDELITY: $F = \langle\Psi^{\perp}|\ \rho_{out}\ |\Psi^{\perp}\rangle$

$= 2/3 = 0.666 = (N+1)/(N+2)$

$= R_{AC}/(2\ R_{AC}+1)$

= independent of output M !

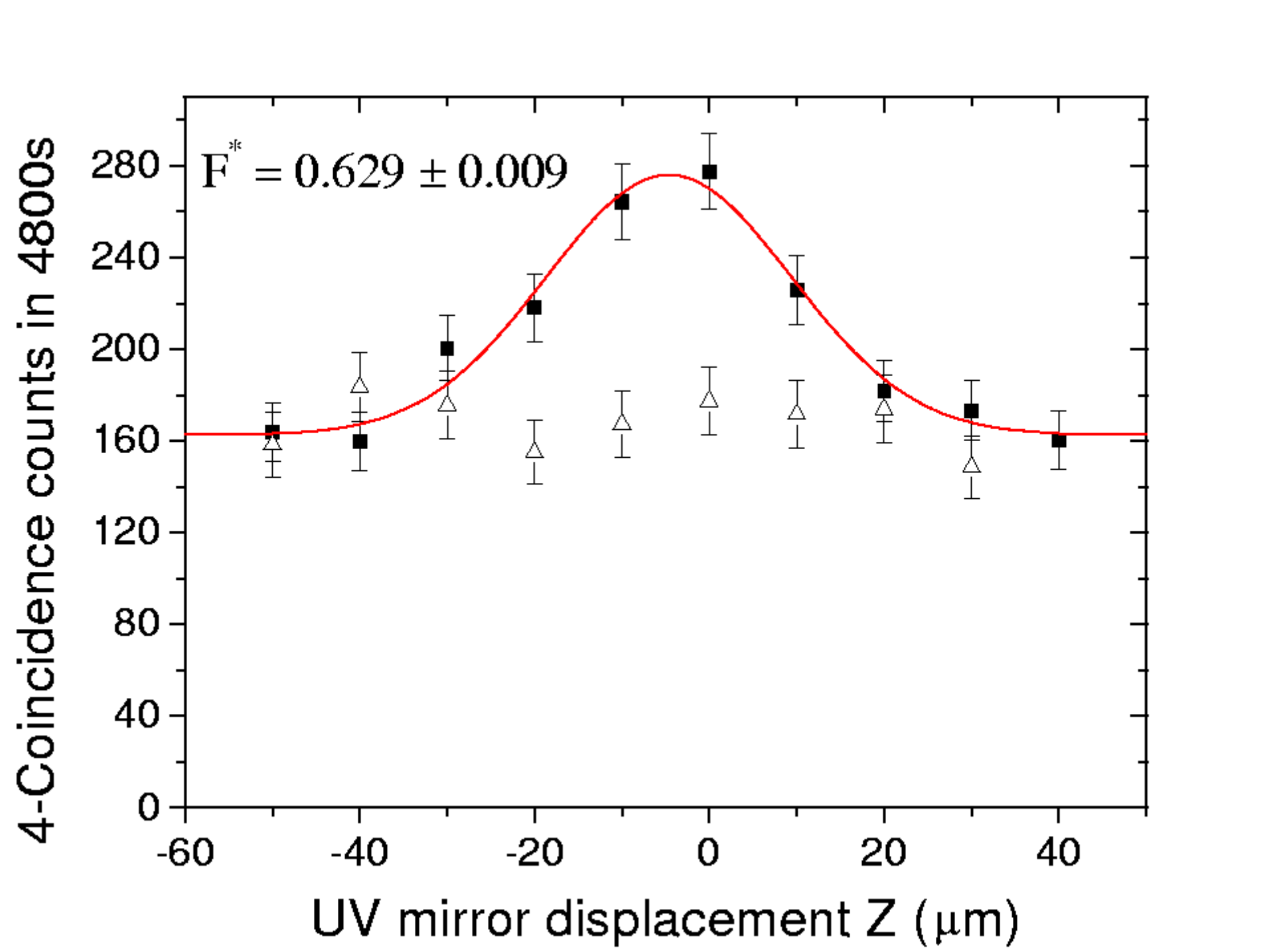
$R_{AC} = 2$: **Probability ratio of detecting 1 particles with expected $\perp$ polarization (π) against detecting it with " wrong" (π)' on the Anti-Cloning channel viz: on output mode k_2**

QUANTUM NOT-GATE

- INJECTION OF N=1 PHOTONS ON INPUT MODE K_1 WITH VERTICAL (V) POLARIZATION
- DETECTION OF M-N=1 PHOTONS ON OUT MODE K_2 (AC) WITH (H) POLARIZATION

FIDELITY: $F_{theor.} = 0.666 = 2/3$

$F_{exp.} = 0.629 \pm 0.009$


$F^{*} = 0.629 \pm 0.009$
4-Coincidence counts in 4800s
0
40
80
120
160
200
240
280
-60
-40
-20
0
20
40
UV mirror displacement Z (μm)

Contextual realization of No-Cloning and U-NOT Gate by the *same* apparatus

NOTE:

NO-Cloning because QM is a *linear-map*

NO U-Not gate because QM is a *CP-map*

BUT: linearity and *CP* are totally *distinct* properties of any quantum map, i.e. a process realizable by Nature.

Any hidden sub-structure in axiomatic Q.theory ?